COHELAN KHOURY & SINGER
Timothy D. Cohelan, Esq. (SBN 60827)
tcohelan@ckslaw.com
Isam C. Khoury, Esq. (SBN 58759)
ikhoury@ckslaw.com
605 C Street, Suite 200
San Diego, CA 92101
Telephone: (619) 595-3001/Facsimile: (619) 595-3000

KEEGAN & BAKER, LLP
Patrick N. Keegan, Esq. (SBN 167698)
pkeegan@keeganbaker.com
2292 Faraday Avenue, Suite 100
Carlsbad, CA 92008
Telephone: (760) 929-9303/Facsimile: (760) 929-9260

Attorneys for Plaintiff JOHN DEDDEH

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JOHN DEDDEH, individually and on behalf of class of similarly situated individuals, Plaintiff, v. POLITICO LLC; Defendants.	Case No. **CLASS ACTION COMPLAINT FOR DAMAGES** **JURY TRIAL DEMANDED**

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Plaintiff John Deddeh, on behalf of himself and a class of similarly-situated individuals as defined below, and based on personal knowledge where applicable, information and belief, and investigation by counsel, allege the following against Defendant Politico LLC ("Defendant" or "Politico").

INTRODUCTION

1. This class action lawsuit arises out of Defendant's policy and practice during the proposed Class Period (i.e., the applicable limitations period preceding the filing of the Complaint in this matter and through and including June 30, 2024) of embedding and using various trackers on Defendant's website, www.Politico.com, to (1) install and store third-party tracker cookies on website users' browsers and (2) collect website users' browser and device data as well as personally identifying information, such as IP addresses,[1] that the Politico website then surreptitiously discloses to and shares with the third-party trackers. Defendant did all of this without users' knowledge, authorization, or consent.

2. Defendant Politico LLC is an American digital newspaper company that owns and operates the www.Politico.com website (the "Politico website"). While primarily providing distributed news, analysis, and opinion online, Politico also produces printed newspapers, radio programming, and podcasts. In October 2021, Defendant was acquired by and now is a subsidiary of Axel Springer SE.

3. Launched in 2007, the Politico website covers politics and policy in the United States and internationally. It has publications dedicated to politics in the United States, the European Union, the United Kingdom Canada, and other countries.

4. Politico touts itself as "the global authority on the intersection of politics, policy, and power." According to its website, Politico "strives to be the dominant source for news on politics and policy in power centers across every continent where access to reliable information, nonpartisan journalism and real-time tools create, inform and engage a global citizenry."

[1] IP addresses have been classified by the United States Department of Health and Human Services ("HHS") as personally identifying information. *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. Department of Health and Human Services (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

5. Plaintiff and Class Members who visited the Politico website during the proposed Class Period expected that their personally identifying information, including their IP addresses, would remain private and confined to their use of the Politico website. Plaintiff and Class Members had a reasonable expectation that their accessing of and interactions with the Politico website during the proposed Class Period would not be shared with any third parties, let alone to undisclosed third-party trackers, or sold for advertising purposes.

6. Unbeknownst to individuals entering and viewing the Politico website during the proposed Class Period, third-party trackers were embedded into Defendant's website. Through that embedded tracking technology, while Plaintiff and Class Members were accessing and interacting with the Politico website, Defendant (1) installed and stored third-party tracker cookies on users' browsers and (2) captured Politico website users' browser and device data, IP addresses, and other identifying information. All of this happened the moment users entered the Politico website and without any further action required by or requested of the users. And it happened without any meaningful notice.

7. Plaintiff is informed and believes, and on that ground alleges, that Defendant surreptitiously shared identifying data, including addressing information such as IP addresses, with the third-party trackers for advertising and analytics-related purposes. Defendant did so without obtaining Politico website users' authorization or consent and without a court order.

8. Defendant's unauthorized (1) installation of third-party tracker cookies on users' web browsers and (2) collection and disclosure to third parties of Plaintiff's and Class Members' personally identifying and addressing information, all without consent or adequate notification to Plaintiff and Class Members, were invasions of Plaintiff's and Class Members' privacy. Defendant's actions also violated multiple laws, including the California Computer Data Access and Fraud Act, Cal. Penal Code § 502 ("CDAFA"); the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA"); and the right to privacy under Article 1, § 1, of the California Constitution, which includes privacy as one of six fundamental rights of all Californians.

///

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

PARTIES

A. Plaintiff John Deddeh

9. Plaintiff John Deddeh is a natural person and a resident of California. While physically present in California, Plaintiff used an internet browser on his computer and on his cellular phone to access Defendant's Politico website on several occasions during the last three years to browse news headlines and to read articles.

10. At no time during the proposed Class Period when Plaintiff entered the Politico website and viewed its contents did he authorize or consent to Defendant installing third-party tracker cookies on his internet browser or computer. Plaintiff also did not consent to Defendant sharing or selling his browser and device data, IP addresses, and other personally identifying information with or to third-party trackers. Further, because Defendant did not provide notice or request permission, Plaintiff was unaware of and had no meaningful opportunity to opt out of or object to that unauthorized disclosure of his data.

B. Defendant and its Politico Website

11. Defendant Politico LLC is a limited liability company organized under the laws of the State of Delaware with its headquarters in Arlington, Virginia. Defendant systematically and continuously does business in California and with California residents.

12. Defendant currently owns and operates the www.Politico.com website, which publishes news focused on global and American politics.

13. During the proposed Class Period, Defendant's Politico website failed to put visitors on notice of Defendant's use of website tracking technology, including its use of third-party trackers. Upon information and belief, Plaintiff alleges that third-party trackers allow companies like and including Defendant to sell advertising space on their websites by using the tracking technology to receive, store, and analyze information collected from website visitors.

14. During the proposed Class Period, the Politico website also failed to disclose the selling and sharing of browser and device data and personally identifying information, including IP addresses and other addressing information, to and with unauthorized third party-trackers for advertising and other purposes.

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d). Specifically, this action satisfies all requirements for federal jurisdiction under CAFA since the allegations in this Complaint identify a putative class of more than 100 members, establish the minimum diversity of citizenship required under CAFA, and put in controversy more than $5 million in the aggregate for the entire class, exclusive of interest and costs. 28 U.S.C. §§ 1332(d), (d)(5), and 1453(b).

16. This Court has personal jurisdiction over the parties because Defendant has sufficient minimum contacts with this State in that it operates and markets its services throughout the State. Further, a substantial part of the events and conduct giving rise to Plaintiff's claims occurred in the State of California. Those events and that conduct included Plaintiff's accessing of the Politico website; Defendant's unauthorized installation of third-party tracker cookies on Plaintiff's web browsers; and the collection and surreptitious sharing of browser and device data and personally identifying information with the third-party trackers, all without users' knowledge, authorization, or consent. Plaintiff's rights were violated in the State of California, and those violations arose out of his contact with Defendant from and within California.

17. Venue is proper in this Court because on information and belief, Defendant Politico LLC is a foreign business entity and, as of the date on which this Complaint was filed, had failed to designate a principal place of business in California with the office of the Secretary of State.

18. Article III standing is met when a plaintiff "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 337, 338 (2016).

19. Plaintiff meets the "injury in fact" requirement because their invasion of privacy is a "concrete and particularized" injury. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2204 (2021) ("Various intangible harms can also be concrete [including] . . . disclosure of private information"); *In re Facebook Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir.

2020) (holding that Facebook's tracking of browsing histories that were sold to advertisers was an "invasion of [a] legally protected interest that is concrete and particularized."). Plaintiff alleges that he was personally injured when Defendant impermissibly obtained Plaintiffs' personal information. It is black-letter law that such allegations are sufficient to confer Article III standing. *See, e.g., Mastel v. Miniclip SA*, 2021 WL 2983198, at *6 (E.D. Cal. July 15, 2021) (collection of "personal information without the plaintiff's consent involve a sufficiently 'concrete' injury"); *In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F.Supp.3d 767, 784 (N.D. Cal. 2019) (dissemination to third parties of plaintiffs' personal information is "sufficient to confer [Article III] standing.") Separate from an invasion-of-privacy harm, Plaintiff also alleges economic harm sufficient for Article III standing by alleging user data carries financial value, citing a study that values user data at a quantifiable number; and allegations that Defendant profited from the data. The Ninth Circuit has found that such allegations are sufficient to establish Article III standing under a theory of economic harm. *See Facebook Tracking*, 956 F.3d at 600. Further, "[u]nder California law, this stake in unjustly earned profits exists regardless of whether an individual planned to sell his or her data or whether the individual's data is made less valuable." *Facebook Tracking*, 956 F.3d at 600. Plaintiffs' injury is "fairly traceable" to Defendant's challenged conduct, *Spokeo*, 578 U.S. at 338, because Plaintiff's private information was acquired by Defendant through the use of third-party trackers are embedded into Defendant's website. Thus, Plaintiff's injury thus occurred at the moment his information was improperly acquired by Defendant. Plaintiff meets the redressability element because courts have consistently recognized that violation of privacy rights can be redressed by an award of damages or injunctive relief. *See Facebook Privacy*, 402 F.Supp.3d at 784 ("[T]he Ninth Circuit has repeatedly explained that intangible privacy injuries can be redressed in the federal courts."); *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 912 (9th Cir. 2011) (similar). Additionally, the injunctive relief Plaintiff seeks includes terminating all downstream distributions of such personal data illegally collected, which would redress future harms suffered by Plaintiff and the Class.

///

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

20. Plaintiff adequately alleges statutory standing to bring California Invasion of Privacy Act ("CIPA") claim against the Defendant website owner arising from website's downloading of software "trackers" onto Plaintiff's web browser, constituting unauthorized "pen registers" under CIPA, where Plaintiff alleges that collection of his internet protocol ("IP") addresses through the trackers allowed third parties to obtain personally identifying, non-anonymized information, that IP addresses revealed geographical location and other personal information sufficient for third parties to conduct targeted advertising, that Plaintiff was unaware of the tracking, and that Plaintiff did not consent to it. *Shah v. Fandom, Inc.*, 2024 WL 4539577 (N.D. Cal., Oct. 21, 2024, No. 24-CV-01062-RFL).

FACTUAL ALLEGATIONS COMMON TO THE CLASS

A. Website Tracking Technology

21. Trackers collect information about internet users as those users browse the web. Trackers use cookies, scripts, or pixels inserted by publishers or advertisers. Tracker profiling is the process of linking data from different websites to build user profiles based on browsing history, to place users in groups, and to sell that data to third parties for targeted advertising.

22. There is a broad range of online technologies that track and monitor internet-based interactions and communications. Four identifier tools commonly used are (i) website cookies, (ii) tracking pixels, (iii) digital fingerprinting, and (iv) software development kits.

23. A website cookie refers to a small text file that a website server creates and transmits to a web browser (e.g., Chrome or Safari) which then installs and stores the file in a particular directory on an individual's computer, phone, or other device.[2] When a website user attempts to access a webpage, the user's browser transmits a communication to the website's server requesting that the server display the website's content for the browser to load. While providing the requested content to the user, the website's server also provides the cookies that it would like the user's browser to install and retain.

24. Website cookies contain information that identifies the domain name of the webserver that wrote the cookie (e.g., hulu.com or facebook.com). Cookies also have

[2] See Sara J. Nguyen, *What Are Internet Cookies and How Are They Used?*, All About Cookies (Jul. 28, 2023), https://allaboutcookies.org/what-is-a-cookie.

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

information about the user's interaction with a website, such as how the website should be displayed, how many times a user has visited the website, how long a user spends on a webpage, information about what pages the user visited, and authentication information. In addition to a unique identifier and a site name, website cookies also can include personally identifiable information such as a user's name, address, email or telephone number if that information was provided to a website.

25. A first-party cookie is implemented by the website that the user accesses. The website uses its cookies for authentication, monitoring user sessions, and collecting analytical data. A third-party cookie, also called an "advertising cookie" or a "tracker cookie," is a cookie that belongs to a domain other than the one being displayed to the user in his or her browser. A third-party cookie typically is used for cross-site tracking, retargeting, and ad-serving. The key differences between the first- and third-party cookies are who sets them (i.e., a website display host or a third party), whether and how they can be blocked by a web browser, and the availability of the cookie. A third-party advertising or tracker cookie is accessible on any website that loads the third-party server's code.

26. A pixel, also known as a "tracking pixel," "web bug," "clear GIF," or "web beacon," is similar to a website cookie, and is a small, almost-invisible image (pixel) embedded in a website or an email to track a user's activities. That tracked data often includes the user's operating system, the type of website or email used, the time when the website was accessed, the user's IP address, and whether there are cookies that previously have been set by the server hosting the pixel image.[3]

27. Digital fingerprinting refers to device fingerprinting and browser fingerprinting, both of which send information to the website server to help ensure that a website is displaying content and operating appropriately. Although a browser or device does not usually transmit personal information about a user, most fingerprinting is performed via a third-party tracker,

[3] See Patti Croft & Catherine McNally, *What Is a Web Beacon and Why Should You Care?*, All About Cookies (Sept. 26, 2023), https://allaboutcookies.org/what-is-a-web-beacon.

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

which can track an individual across multiple sites and form a profile of the user.[4]

28. A software development kit ("SDK") is a set of computer programs and similar tools that developers and engineers can leverage to build applications for specific platforms. The SDK often includes, among other tools, libraries, application programming interfaces, instructions, guides, directions, and tutorials.[5] SDKs also may have embedded code that allows them to intercept personal data and other information from application users surreptitiously, including geolocation data, usernames and communications derived from other SDK applications installed on a user's device, and a user's activities within an application after installation.

29. All of the information and data captured and collected by third-party trackers, regardless of the tool used, can be sold and used for marketing and advertising purposes.

B. Internet Protocol Addresses ("IP Addresses")

30. One important piece of identifying information collected by third-party trackers is a website user's IP address. An IP address is a unique identifier for a device, which is written as four sets of numbers separated by periods (e.g., 123.145.167.189). The first two sets of numbers reflect what network the device is on, and the second two sets of numbers identify the specific device. The IP address enables a device to communicate with another device, such as a computer's web browser communicating with a website server.

31. Similar to a telephone number, an IP address is a unique numerical code associated with a specific internet-connected device on a computer network. The IP address identifies all of the devices accessing a certain network at any given time.

32. Significantly, an IP address contains geographical location information from which the state, city and zip code of a specific device can be determined. Given the information that it can and does reveal, an IP address is considered personally identifiable information and

[4] See Anokhy Desai, *The Half-Baked Future of Cookies and Other Tracking Technologies*, IAPP (July 2023), https://iapp.org/resources/article/future-of-cookies-tracking-technologies/.

[5] *What Is an SDK? Software Development Kits Explained*, Okta, Inc. (June 30, 2022), https://www.okta.com/identify-101/what-is-an-sdk.

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

is subject to HIPAA protection.[6]

33. Knowing a website user's IP address, and therefore the user's geographic location, provides "a level of specificity previously unfound in marketing."[7] An IP address allows advertisers to target customers by countries, cities, neighborhoods, and postal code.[8] Even more specifically, it allows advertisers to target specific households, businesses, and even individuals with ads that are relevant to their interests.[9]

34. Indeed, IP targeting is one of the most successful marketing techniques that companies can employ to spread the word about a product or service because companies can use an IP address to identify individuals personally.[10] By targeting specific households or businesses, a company can avoid wasting money on ads that are unlikely to be seen by their target audience and can reach their target audience with greater precision.[11] Additionally, by analyzing data on which households or businesses are responding to their ads, IP address targeting can help businesses improve their overall marketing strategy and refine their marketing efforts.[12]

35. As alleged below, Defendant installed third-party tracker cookies on Politico website users' browsers. Those trackers have collected browser and device data as well as identifying and addressing information about Plaintiff and Class Members, including their IP addresses, all without a court order or consent.

C. Defendant's Use of Third-Party Trackers on the Politico Website

36. Defendant has embedded and implemented several third-party trackers on the

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

---

[6] *See* 45 C.F.R. § 164.514(b)(2)(i)(O).

[7] *IP Targeting: Understanding This Essential Marketing Tool*, AccuData, https://www.accudata.com/blog/ip-targeting/ (last visited April 17, 2024).

[8] *Location-based Targeting That Puts You in Control*, Choozle, https://choozle.com/geotargeting-strategies/ (last visited April 17, 2024).

[9] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf/

[10] Trey Titone, *The future of IP address as an advertising identifie*r, Ad Tech Explained (May 16, 2022), https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

[11] Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LinkedIn (Nov. 29, 2023), https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf/

[12] *Id*.

Politico website, including but not limited to (i) TripleLift Tracker, (ii) CasaleMedia Tracker and (iii) Adnx Tracker (the "trackers"). By installing those trackers and their corresponding tracking cookies, Defendant can sell advertising space on the Politico website, enabling Defendant to monetize its website further and earn additional revenue. Moreover, by collecting and disclosing its users' information, Politico can place advertisements on other companies' websites, thereby increasing its own brand awareness and sales and enabling Defendant to obtain and analyze users' data for its own profit.

37. When a website user first accesses and enters the Politico website, the user's browser sends an HTTP request to Defendant's server. The Politico website server then sends an HTTP response with directions to load the webpage content and to install the three trackers on the user's browser.

38. Each tracker installs and stores its own website cookie on the user's browser and uses that third-party tracker cookie to collect and share that user's browser and device data and addressing information, including IP addresses, every time the user visits and interacts with the Politico website.

39. The process described above takes place behind the scenes and in less than a second. Thus, the three tracker cookies appear and are implemented the instant the user enters the Politico website, without any further action, clicks, or consent required by the user.

40. Further, each of the three trackers embedded on Defendant's website re-installs its tracker cookies every time a user visits the Politico website. Thus, even if a user clears the cookies from the user's browser, it makes no difference: the next time that user visits the Politico website, all three trackers re-install their tracker cookies, reset the tracking process, and resume transmission of the user's browser and device data, IP address, and other identifying information to the undisclosed third parties.

41. The TripleLift Tracker is developed by digital advertising company TripleLift, Inc. ("TripleLift"). TripleLift is a platform that seeks to enhance advertisers' performance. To increase the overall effectiveness of online advertising, the TripleLift Tracker focuses on collecting users' data, particularly IP addresses, to fine-tune the platform's ad targeting.

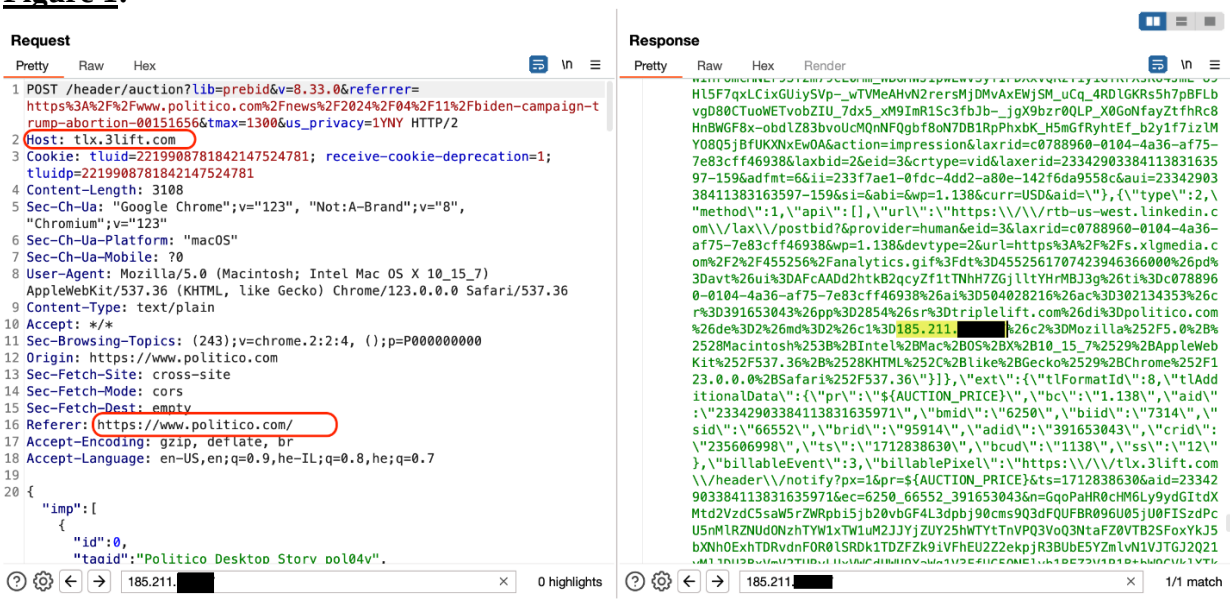
COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

TripleLift's approach integrates both third-party and first-party data through its "TripleLift Audiences" feature, which facilitates precise ad placements and maximizes the accuracy of the advertisement's targeting. In essence, the TripleLift Tracker enables websites to analyze users' data to craft and optimize marketing campaigns, to target specific user groups and to increase website revenue by facilitating the collection of website users' information for use by third-parties.

42. When a user visits the Politico website, the TripleLift Tracker installs and stores its website cookie on the user's browser. This third-party tracker cookie is used to collect and share that user's browser and device data, IP address, and other identifying information with third-party TripleLift. That, in turn, enables TripleLift to serve personalized advertisements and optimize user engagement. TripleLift receives a user's data and IP address each and every time the user interacts with the Politico website. See Figure 1.

Figure 1:



43. The CasaleMedia Tracker is developed by Index Exchange, Inc. ("Index Exchange"), formerly known as Casale Media. By integrating third-party and first-party data, Index Exchange seeks to maximize ad relevancy and placement precision by leveraging the company's advertising technology experience for publishers, advertisers, and consumers within its global advertising marketplace. The CasaleMedia Tracker collects user data, including browser and device data and IP addresses, to enable website owners to analyze user data

thoroughly, target specific user demographics, and optimize their marketing campaigns by increasing advertising effectiveness. By continuously updating its data sets to refine ad targeting, the CasaleMedia Tracker allows for the strategic collection of users' information for use by third-parties that purchase the information.

44. Politico embeds Index Exchange's code on its website. That hidden code enables Index Exchange to install and store the CasaleMedia Tracker and its corresponding website cookie on users' browsers. Like the TripleLift Tracker above, the CasaleMedia Tracker is installed the instant a user accesses the Politico website. That happens without any notice to or request for permission from the user. By using HTTP requests and responses, cookies, IP addresses, and other information shared by the Politico website, third-party Index Exchange can track and deliver personalized ads based on users' browsing habits and preferences, geographic locations, and other data personal to the users.

45. During the HTTP communication process, the CasaleMedia tracker cookie stores identifiers linked to users' browsing behavior. That enables Index Exchange to recognize that user on the user's subsequent visits to Politico or to other websites within Index Exchange's advertising network. That, in turn, facilitates a cycle of ad targeting and tracking.

46. Index Exchange also receives a user's browser and device data and IP address every time the user interacts with the Politico website. If cookies are cleared from the user's browser, the CasaleMedia Tracker is re-installed instantly on the user's next visit to the Politico website. This automatic process ensures that Index Exchange consistently receives the user's data and IP address with each website interaction. See Figure 2.

///

///

///

///

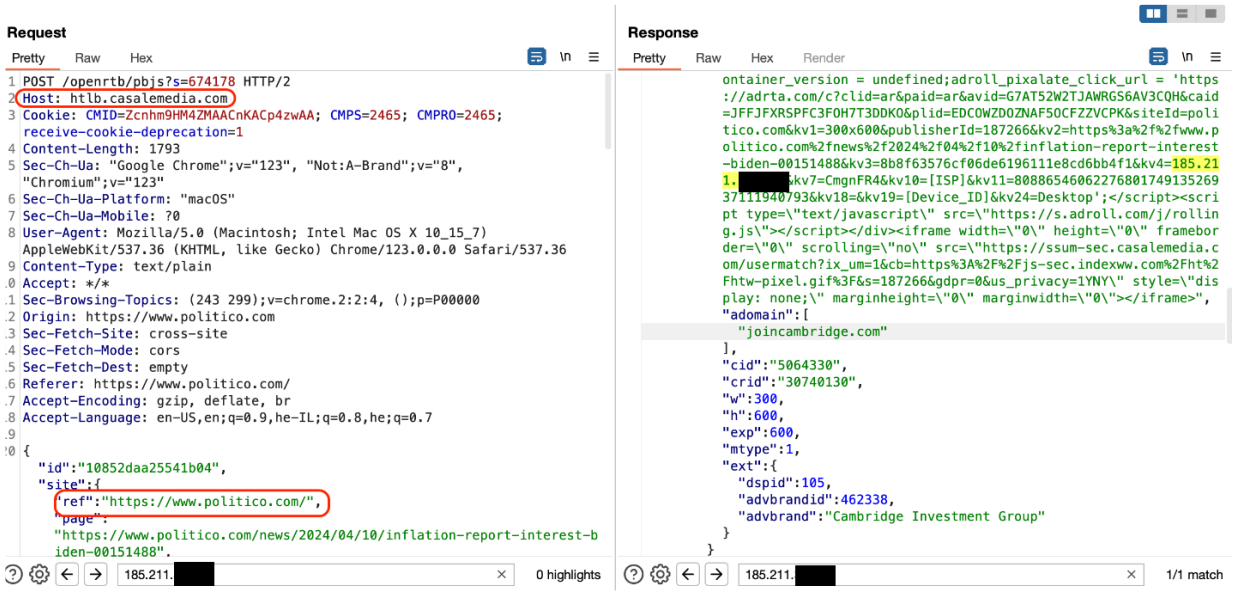
///

///

///

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Figure 2:



47. The third tracker embedded in Defendant's Politico website is developed by software company Xandr, which Microsoft acquired in 2021. Xandr operates as an advanced advertising company that claims to provide a comprehensive platform for buying and selling consumer-oriented digital advertising. The platform, which includes programmatic advertising, data analytics, and cross-screen media solutions, claims to improve the efficiency and effectiveness of advertising across various channels by leveraging data and technology.

48. Like other third-party trackers, Xandr allows companies like Defendant to sell advertising space on their websites by using the Adnx Tracker to receive, store and analyze information collected from website visitors. The Adnx Tracker is installed and stored on the user's browser the instant the user enters the Politico website. The third-party tracker cookie then sends the user's IP address to Xandr each and every time the user interacts with the Politico website. See Figure 3.

///

///

///

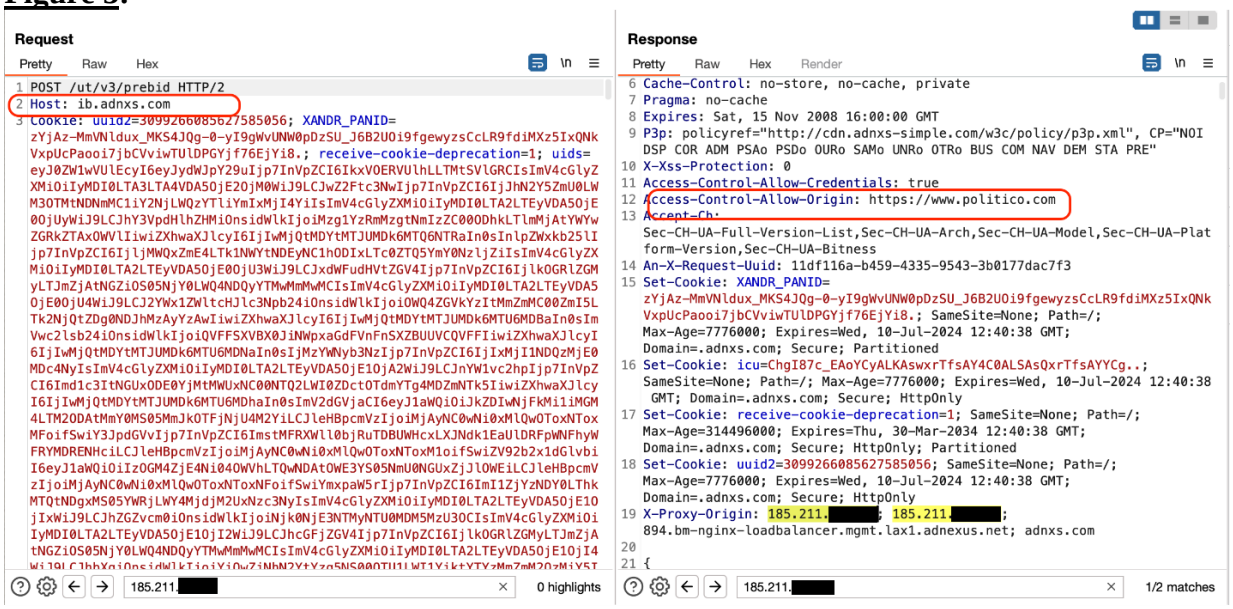
///

///

///

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Figure 3:



49. During the proposed Class Period, each of the three trackers embedded on Defendant's Politico website (1) installed a third-party tracker cookie on users' browsers and (2) captured, collected, and shared with undisclosed third parties the Politico website users' personally identifying and addressing information, including the users' IP addresses, all without users' knowledge or consent.

50. Upon further information and belief, all three trackers were used for real-time bidding ("RTB"). Essentially, when a user entered the Politico website, an advertising auction took place almost instantly. Defendant's website used the third-party trackers to "host" the bidding on Defendant's behalf. The RTB system was designed to allow Defendant to sell targeted advertising and to maximize its revenue gained from selling ad space on the Politico website.

51. Further, each of the three trackers embedded on Defendant's website re-installed its tracker cookies instantly every time a user visited the Politico website. That happened even if the user previously cleared the cookies from his or her web browser. As a result, during the proposed Class Period, Politico website users could not escape the unauthorized sharing of their personally identifying and addressing information with third-parties TripleLift, Index Exchange, and Xandr.

///

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

D. Plaintiff and Class Members Did Not Consent to Defendant's Disclosure of Their Personally Identifying and Addressing Information, and They Have a Reasonable Expectation of Privacy in Their User Data

52. During the proposed Class Period, Defendant did not ask its Politico website visitors, including Plaintiff, whether they consent to having their personally identifying and addressing information disclosed to and used by third parties like TripleLift, Index Exchange, and Xandr. When a website user accessed and entered the Politico website during the proposed Class Period, there was no pop-up window or other notification to inform users that Defendant was using website tracking technology or installing third-party tracker cookies.

53. Additionally, the third-party trackers were incorporated seamlessly – and, to users, invisibly – in the background on the Politico website. That seamless and invisible incorporation gave Plaintiff and Class Members no way of knowing that Defendant was collecting their personally identifying and addressing information, including their IP addresses, and secretly sharing that information with undisclosed third parties.

54. Further, although the Politico website does have a Privacy Policy containing some disclosures about how information is shared, that policy can be viewed only after scrolling through all the website content to the very bottom of the webpage. During the proposed Class Period, Defendant's policies and notices would be seen, if at all, only long after the third-party trackers and cookies had been installed on users' web browsers – in other words, only after it was too late.

55. In addition to its hard-to-see location, the hyperlink to access the Privacy Policy is written in small, inconspicuous font and is listed among a number of other links at the bottom of the Politico webpage. See Figure 4.

Figure 4:

56. Unlike first-party cookies that may be technologically necessary to enable a computer user to view a webpage, third-party tracker cookies are not necessary. Moreover, they

(1) simultaneously communicate information to an external server as a user navigates a website; (2) track users across devices, meaning that a user's actions on multiple devices all will be included in the information stored regarding that user; (3) are not easily disabled by users; and/or (4) create a record of all of the information that users provide to and/or receive from the website. Because they were unaware of Defendant's use of third-party trackers and tracking cookies, Plaintiff and Class Members could not and did not consent to the collection, storage, and use of their personally-identifying and addressing information by undisclosed third parties like TripleLift, Index Exchange and Xandr.

57. During the proposed Class Period, Plaintiff and Class Members had a reasonable expectation of privacy in their interactions with the Politico website and their user data, especially their personally identifying information. This is even truer of Plaintiff's and Class Members' IP addresses, which contain geolocation data that can be used to identify, track, and target individuals in a very specific way.

58. Privacy studies, such as those conducted by the Pew Research Center, show that most Americans are concerned about how data is collected about them.[13] Those privacy polls also reflect that Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares data regarding that customer or other individual.

59. Indeed, according to Consumer Reports, more than 90% of Americans believe that more should be done to ensure that companies protect consumers' privacy. Further, a supermajority of Americans – 64% – believe that companies should be prohibited from sharing data with third parties, while 63% of Americans want a federal law requiring companies to obtain a consumer's permission before sharing the consumer's information. To that end, 60% of Americans believe that companies should be required to be more transparent about their

[13] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,* Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

privacy policies so that consumers can make more informed choices.[14]

60. Users act in a manner that is consistent with those preferences. During a rollout of new iPhone operating software, for example, 94% of U.S. users who were asked for clear, affirmative consent before allowing companies to track them chose not to share their data.[15]

61. Defendant's unauthorized (1) installation of third-party tracker cookies on Plaintiff's and Class Members' web browsers and (2) collection and disclosure of Plaintiff's and Class Members' personally identifying and addressing information to undisclosed third parties, all without any consent or even adequate notification, were invasions of Plaintiff's and Class Members' privacy.

62. Plaintiff and Class Members have suffered injuries in the form of (i) invasion of privacy; (ii) statutory damages; (iii) the continued and ongoing risk to their personally identifying information that, once out, never can be restored to its previous level of privacy; and (iv) the continued and ongoing risk of harassment, spam and targeted advertisements enabled by the Politico website.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this action under Federal Rules of Civil Procedure 23 on behalf of himself and a class (the "Politico Website Class" or "the Class") defined as follows:

> All California residents who, while located within California at any time during the applicable limitations period preceding the filing of the Complaint in this matter, accessed and viewed the Politico website and had their IP addresses and/or browser and device data collected by and disclosed to the third-party trackers embedded in the Politico website.

64. Excluded from the Politico Website Class are website users who (i) registered and/or subscribed to the Politico website and/or (ii) registered to receive the Politico newsletter. Employees of Defendant and employees of Defendant's parents, subsidiaries, and corporate affiliates also are excluded from the Class. Plaintiff reserves the right to amend or modify the

[14] Benjamin Moskowitz et al., *Privacy Front & Center: Meeting the Commercial Opportunity to Support Consumer Rights*, Consumer Reports in collaboration with Omidyar Network (Fall 2020), https://thedigitalstandard.org/downloads/CR_PrivacyFrontAndCenter_102020_vf.pdf

[15] See https://www.wired.co.uk/article/apple-ios14-facebook ("According to Flurry Analytics, 85 per cent of worldwide users clicked 'ask app not to track' when prompted, with the proportion rising to 94 per cent in the US.").

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

class definition and/or to add sub-classes or limitations to particular issues, where appropriate, based upon subsequently discovered information.

65. This action properly may be maintained as a class action under Federal Rules of Civil Procedure because (1) there is a well-defined community of interest in the litigation, (2) common questions of law and fact predominate over individual issues, and (3) the proposed Class is ascertainable.

Numerosity

66. The Politico Website Class that Plaintiff seeks to represent contains numerous members and is clearly ascertainable including, without limitation, by using Defendant's records and/or third-party trackers' records to determine the size of the Class and to determine the identities of individual Class Members.

67. Based on information and belief, the Politico Website Class consists of at least 75 individuals. The Class is so numerous that joinder of all members is impracticable.

Typicality

68. Plaintiff's claims are typical of the claims of all the other members of the Politico Website Class as Plaintiff has suffered from the same violations of the law as other putative Class Members. Plaintiff's claims and the Class Members' claims are based on the same legal theories and arise from the same unlawful conduct, resulting in the same injury to Plaintiff and all of the other Class Members.

Adequacy

69. Plaintiff will fairly and adequately represent and protect the interests of the other members of the Class. Plaintiff has retained competent counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and his counsel are committed to prosecuting this action vigorously on behalf of the Politico Website Class Members and have the financial resources to do so. Neither Plaintiff nor his counsel have any interests that are adverse to those of the other Politico Website Class Members.

Commonality and Predominance

70. By its unlawful actions, Defendant has violated Plaintiff's and the Class

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Members' rights under the CDAFA, the CIPA, and the California Constitution. The questions raised are, therefore, of common or general interest to the Class Members, who have a well-defined community of interest in the questions of law and fact presented in this Complaint.

71. This action involves common questions of law and fact that predominate over any questions affecting only individual Class Members. Those common questions of law and fact include, without limitation, the following:

(a) Whether Plaintiff and Class Members had a reasonable expectation of privacy when they accessed and visited the Politico website during the proposed Class Period;

(b) Whether Defendant knowingly and without permission accessed Plaintiff's and Class Members' computers during the proposed Class Period;

(c) Whether Defendant knowingly and without permission altered, damaged, deleted, destroyed, or otherwise used any data from Plaintiff's and Class Members' computers during the proposed Class Period;

(d) Whether Defendant knowingly and without permission took, copied, or made use of any data from Plaintiff's and Class Members' computers during the proposed Class Period;

(e) Whether Defendant knowingly and without permission added, altered, damaged, deleted, or destroyed any data from Plaintiff's and Class Members' computers during the proposed Class Period;

(f) Whether Plaintiff and Class Members had a reasonable expectation of privacy in their personally identifying information, including IP addresses, when they accessed and visited the Politico website during the proposed Class Period;

(g) Whether each of the third-party trackers embedded in the Politico website was a "pen register" under California Penal Code § 638.50(b);

(h) Whether, during the proposed Class Period, Defendant had a policy or practice of collecting and sharing personally identifying and addressing information collected on the Politico website including, without limitation, IP addresses and/or browser and device data, with third-party trackers and/or other third parties;

(i) Whether, during the proposed Class Period, Defendant had a policy or practice of not disclosing to Politico website users that it would collect and share their personally identifying and addressing information, including IP addresses and/or browser and device data, with third-party trackers and/or other third parties;

(j) Whether, during the proposed Class Period, Defendant had a policy or practice of not obtaining Politico website users' prior consent to collect and share personally identifying and addressing information, including IP addresses and/or browser and

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

device data, with third-party trackers and/or other third parties;

(k) Whether Defendant sought or obtained a court order for its use of the third-party trackers;

(l) Whether Defendant's conduct invaded Plaintiffs' and Class Members' privacy;

(m) Whether Defendant's acts and practices violated California's Computer Data Access and Fraud Act, Cal. Penal Code § 502;

(n) Whether Defendant's acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code § 638.51(a);

(o) Whether Defendant's acts and practices violated the California Constitution or individual rights arising under the California Constitution; and

(p) Whether Plaintiff and Class Members are entitled to actual, statutory, nominal, and/or other forms of damages, restitution, and other relief.

Superiority

72. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all of the members of the Class is impracticable and because questions of law and fact common to the Politico Website Class predominate over any questions affecting only individual members of the Class. Even if every individual member of the Class could afford individual litigation, the court system could not. It would be unduly burdensome to the courts if individual litigation of the numerous cases were to be required. Individualized litigation also would present the potential for varying, inconsistent or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. By contrast, the conduct of this action as a class action with respect to some or all of the issues will present fewer management difficulties, conserve the resources of the court system and the parties, and protect the rights of each member of the Politico Website Class. Further, it will prevent the very real harm that would be suffered by numerous members of the putative Class who simply will be unable to enforce individual claims of this size on their own, and by Defendant's competitors, who will be placed at a competitive disadvantage as their punishment for obeying the law. Plaintiff anticipates no difficulty in the management of this case as a class

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

action.

73. The prosecution of separate actions by individual members of the Politico Website Class would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other members of the Class who are not parties to those adjudications or that would substantially impair or impede the ability of those non-party members of the Class to protect their interests.

74. The prosecution of individual actions by members of the Politico Website Class also would run the risk of establishing inconsistent standards of conduct for Defendant.

FIRST CAUSE OF ACTION
Violation of the California Computer Data Access and Fraud Act
California Penal Code § 502
(On Behalf of Plaintiff and the Class)

75. Plaintiff incorporates each allegation set forth above as if fully set forth herein and further allege as follows.

76. The California Legislature enacted the CDAFA with the intent to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

77. The Legislature further declared that "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

78. For purposes of the statute, a number of definitions were provided. The term "access" means to "gain entry to, instruct, cause input to, cause output from, cause data processing with, or communicate with, the logical, arithmetical, or memory function resources of a computer, computer system, or computer network." Cal. Penal Code § 502(b)(1).

79. The term "computer program or software" is defined as "a set of instructions or statements, and related data, that when executed in actual or modified form, cause a computer,

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

computer system, or computer network to perform specified functions." Cal. Penal Code § 502(b)(3).

80. The term "computer system" refers to "a device or collection of devices, including support devices and excluding calculators that are not programmable and capable of being used in conjunction with external files, one or more of which contain computer programs, electronic instructions, input data, and output data, that performs functions, including but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." Cal. Penal Code § 502(b)(5).

81. Plaintiff's and Class Members' web browsers used to access the Politico website are "computer software," and the computers on which Plaintiff and Class Members used their web browsers constitute computers or "computer systems" within the scope of the CDAFA.

82. The statute also defines the term "data" to mean a "representation of information, knowledge, facts, concepts, computer software, or computer programs or instructions." The statute further provides that data may be in "any form, in storage media, or as stored in the memory of the computer or in transit or presented on a display device." Cal. Penal Code § 502(b)(8).

83. As discussed above, a website cookie, including a third-party tracker cookie, and an IP address both are "data" within the meaning of the statute.

84. Under California Penal Code § 502(c)(1), it is unlawful to knowingly access and without permission alter, damage, delete, destroy, or otherwise use any data, computer, computer system, or computer network in order to…wrongfully control or obtain money, property or data. Cal. Penal Code § 502(c)(1).

85. The statute also makes it unlawful knowingly to access and without permission take, copy, or make use of any data from a computer, computer system, or computer network. Cal. Penal Code § 502(c)(2).

86. The CDAFA further prohibits any person from knowingly accessing and without permission adding, altering, damaging, or destroying any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

computer network. Cal. Penal Code § 502(c)(4).

87. Under subsections (6) and (7) of Penal Code § 502(c), a person also may not knowingly and without permission (i) provide or assist in providing a means of accessing or (ii) access or cause to be accessed any computer, computer system, or computer network. Cal. Penal Code §§ 502(c)(6) and (7).

88. Based on Defendant's unauthorized installation and storage of third-party tracker cookies on Plaintiff's and Class Members' web browsers during the proposed Class Period, as alleged above, Defendant knowingly accessed and without permission altered and used Plaintiff's and Class Members' data and computer systems in violation of Penal Code § 502(c)(1).

89. Similarly, the installation of those third-party tracker cookies violated Subsection (c)(4) because Defendant added and altered data and computer software on Plaintiff's and Class Members' computers or computer systems. Cal. Penal Code § 502(c)(4).

90. By installing third-party tracker cookies, Defendant also knowingly and without permission provided those trackers a means of accessing and/or caused to be accessed Plaintiff's and Class Members' computers, computer systems, and/or computer networks in violation of Penal Code §§ 502(c)(6) and (7).

91. Further, Defendant's unauthorized collection and disclosure of Plaintiff's and Class Members' personally identifying and addressing information to undisclosed third parties during the proposed Class Period violated Penal Code § 502(c)(2) because Defendant took and made use of data, including IP addresses, from Plaintiff's and Class Members' computers, computer systems, or computer networks.

92. Plaintiff and Class Members are residents of California and used their computers, computer systems, and/or computer networks in California. Defendant accessed or caused to be accessed Plaintiff's and Class Members' data and other personally identifying information from within California.

93. Defendant was unjustly enriched by accessing, acquiring, taking, and using Plaintiff's and Class Members' data and computer systems during the proposed Class Period

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

without their permission or consent and by using all of that identifying information to maximize revenue from selling advertising space on the Politico website for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

94. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiff and Class Members have suffered damages. Under Penal Code § 502(e)(1), Plaintiff and Class Members are entitled to compensatory damages, injunctive relief and other equitable relief in an amount to be determined at trial.

95. Plaintiff and Class Members also are entitled to an award of reasonable attorneys' fees and costs under Penal Code § 502(e)(2).

SECOND CAUSE OF ACTION
Unlawful Use of a Pen Register or Trap and Trace Device
California Penal Code §§ 638.51
(On Behalf of Plaintiff and the Class)

96. Plaintiff incorporates each allegation set forth above as if fully set forth herein and further allege as follows.

97. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq*. ("CIPA"), to address "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id*. § 630. CIPA is intended "to protect the right of privacy of the people of this state." *Id*.

98. Although CIPA was enacted before the dawn of the Internet, the California Supreme Court "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme." *In re Google Inc*., 2013 WL 5423918, at *21 (N.D. Cal. Sept. 26, 2013); *see also Greenley*, 2023 WL 4833466, at *15 (referencing CIPA's "expansive language" when finding that software was a "pen register"); *Javier v. Assurance IQ, LLC*, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [CIPA] Section 631(a) applies to Internet communications."). This is consistent

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

with the observation in *Matera v. Google Inc*. that, "when faced with two possible interpretations of CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection." *Matera v. Google Inc*., 2016 WL 8200619, at *19 (N.D. Cal. Aug. 12, 2016).

99. Particularly pertinent here, California Penal Code § 638.51(a) makes it unlawful for a person to "install or use a pen register or a trap and trace device without first obtaining a court order."

100. A "pen register" is "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." Cal. Penal Code § 638.50(b).

101. A "trap and trace device" is a "a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication, but not the contents of a communication." Cal. Penal Code § 638.50(c).

102. In essence, a "pen register" is a "device or process" that records outgoing information, while a "trap and trace device" is a "device or process" that records incoming information. For example, if a user sends an email, a "pen register" might record the email address from which the email was sent, the email address to which the email was sent, and the subject line – because this is the user's outgoing information. On the other hand, if that same user receives an email, a "trap and trace device" might record the email address from which that email was sent, the email address to which it was sent, and the subject line – because this is incoming information that is being sent to that same user.

103. The three trackers embedded in the Politico website – TripleLift, CasaleMedia, and Adnx – are "pen registers" because each of them is a device or process that captures and records outgoing addressing or signaling information from the electronic communications transmitted by Plaintiff's and Class Members' computers, computer systems, and computer

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

networks as they are accessing and visiting the Politico website.

104. At all relevant times during the proposed Class Period, Defendant installed each of the three pen register trackers on Plaintiff's and Class Members' web browsers and used the trackers to collect Plaintiff's and Class Members' IP addresses and/or browser and device data. IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of the communication. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014).

105. Unaware of Defendant's installation and use of the third-party trackers as pen registers during the proposed Class Period, Plaintiff and Class Members could not have provided and did not provide their prior consent to Defendant's installation or use of the third-party trackers or pen registers.

106. Upon information and belief, Defendant was not authorized by any court order to use a pen register to track Plaintiff's and Class Members' location data and other identifying information.

107. Defendant's conduct as described above violated California Penal Code § 638.51. As a result, Defendant is liable for the relief sought by Plaintiff and the Politico Website Class. Under California Penal Code § 637.2, Plaintiff and Class Members are entitled to and seek statutory damages of $5,000 for each of Defendant's numerous CIPA violations.

THIRD CAUSE OF ACTION
Invasion of Privacy
Violation of Art. 1, § 1, California Constitution
(On Behalf of Plaintiff and the Class)

108. Plaintiff incorporates each allegation set forth above as if fully set forth herein and further allege as follows.

109. "Privacy" is listed in Article I, Section 1, of the California Constitution as one of six fundamental rights of all Californians. That section of the Constitution provides as follows: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

110. The right to privacy in California's Constitution creates a right of action against private entities such as Defendant. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

111. Plaintiff and Class Members had a legally protected privacy interest in their personally identifying information and addressing information that was captured during the proposed Class Period, without notice or consent, when they accessed and viewed the Politico website. These privacy interests are recognized by the California Constitution, CDAFA, CIPA, HIPAA, and numerous other statutes.

112. Plaintiff and Class Members had a reasonable expectation of privacy under the circumstances, as they could not reasonably have expected that Defendant would violate state and federal privacy laws. During the proposed Class Period, Plaintiff and Class Members were not aware of and could not reasonably have expected that Defendant would use website tracking technology and install third-party tracker cookies without notice or obtaining consent. Those unauthorized trackers collected and transmitted to undisclosed third parties Plaintiff's and Class Members' personally identifying and addressing information, including their IP addresses, which contain geolocation data.

113. Defendant's unauthorized (1) installation of third-party tracker cookies and (2) collection and disclosure to third parties of Plaintiffs' and Class Members' personally identifying and addressing information during the proposed Class Period, all without consent or adequate notification to Plaintiff and Class Members, were an invasion of Plaintiff's and Class Members' privacy.

114. Defendant's conduct during the proposed Class Period constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that (i) the information disclosed by Defendant and shared with third-party trackers was personally identifying information protected by the California Constitution and numerous California and federal statutes; (ii) Defendant did not have authorization or consent to disclose that personally

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

identifying and addressing information, including IP addresses, to any third-party tracker embedded in the Politico website, and the trackers did not have authorization to collect and use that geolocation information; and (iii) the invasion deprived Plaintiff and Class Members of the ability to control the dissemination and circulation of that information, an ability that is considered a fundamental privacy right. Defendant's conduct constitutes a severe and egregious breach of social norms.

115. As a direct and proximate result of Defendant's actions, Plaintiff and Class Members have had their privacy invaded and have sustained injury, including injury to their peace of mind.

116. Plaintiff and Politico Website Class Members seek appropriate relief for that injury, including but not limited to restitution, disgorgement of profits earned by Defendant as a result of or in connection with the intrusions upon Plaintiff's and Class Members' privacy, nominal damages, and any and all other equitable relief that will compensate Plaintiff and Class Members properly for the harm to their privacy interests.

117. Plaintiff also seeks such other relief as the Court may deem just and proper.

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

118. Plaintiff incorporates each allegation set forth above as if fully set forth herein and further allege as follows.

119. Defendants received benefits from Plaintiff and Class Members and unjustly retained those benefits at their expense.

120. Plaintiff and Class Members conferred a benefit upon Defendant in the form of valuable personal information and data that Defendant collected from Plaintiff and Class Members, without authorization and proper compensation. Defendant has collected, disclosed, and otherwise misused this information for its own gain, providing Defendant with economic, intangible, and other benefits, including substantial monetary compensation from third parties who received Plaintiff' and Class Members' personal information and data.

121. Defendant unjustly retained those benefits at the expense of Plaintiff and Class

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members.

122. The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles in California and every other state for Defendant to be permitted to retain any of the profit or other benefits they derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

123. Defendant should be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and such other relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION
Violations of California's Unfair Competition Law
Cal. Bus. & Prof. Code §§ 17200, *et seq*.
(On Behalf of Plaintiff and the Class)

124. Plaintiff incorporates each allegation set forth above as if fully set forth herein and further allege as follows.

125. Defendant's business acts and practices are "unlawful" under the California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq*. ("UCL"), because, as alleged above, Defendant violated the California common law, California Constitution, and the other State and Federal statutes and causes of action described herein.

126. Defendant's business acts and practices are "unfair" under the UCL. California has a strong public policy of protecting consumers' privacy interests, including protecting consumers' personal data. Defendant violated this public policy by, among other things, surreptitiously collecting, disclosing, and otherwise misusing Plaintiff' and Class Members' personal information and data without Plaintiff' and Class Members' consent. Defendant's conduct violates the policies of the statutes referenced herein.

127. Defendant's business acts and practices are also "unfair" in that they are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers. The gravity of the harm of Defendant secretly collecting, disclosing, and otherwise misusing

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

Plaintiff's and Class Members' personal information and data is significant, and there is no corresponding benefit resulting from such conduct. Finally, because Plaintiff and Class Members were completely unaware of Defendant's conduct, they could not have possibly avoided the harm.

128. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

129. Had Plaintiff and Class Members known that their information would be collected, and otherwise misused for Defendant's own benefit, they would not have used Defendant's website.

130. Plaintiff and Class Members have a property interest in their sensitive personal data. By surreptitiously collecting and otherwise misusing Plaintiff' and Class Members' information, Defendant has taken property from Plaintiff and Class Members without providing just or any compensation.

131. For these reasons, Plaintiff seeks restitution from Defendant on behalf of himself and Class Members; and injunctive relief in the form of a permanent injunction enjoining Defendant's unlawful and unfair business activities, including an injunction terminating all downstream distributions of Plaintiff's and the Class Members' personal data illegally collected; and any other equitable relief the Court deems proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the members of the Class, prays for the following relief:

a. An order certifying the Politico Website Class, appointing Plaintiff John Deddeh as representative of the Politico Website Class, and appointing counsel for Plaintiff as counsel for the Politico Website Class;

b. An order declaring that Defendant's actions, as described above, violated California Penal Code § 502;

c. An order declaring that Defendant's actions, as described above, violated California Penal Code § 638.51;

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101

d. An order declaring that Defendant's actions, as described above, violated Art. 1, § 1 of the California Constitution;

e. A judgment for and award of compensatory damages or other equitable relief under California Penal Code § 502(e)(1) to Plaintiff and each of the members of the Politico Website Class;

f. A judgment for and award of statutory damages of $5,000 per violation of CIPA under California Penal Code § 637.2 to Plaintiff and each of the members of the Politico Website Class;

g. A judgment for and award of restitution, disgorgement of profits, and nominal damages to which Plaintiff and all of the members of the Politico Website Class are entitled by law;

h. Payment of costs of the suit;

i. Payment of attorneys' fees under California Code of Civil Procedure § 1021.5 and Penal Code § 502(e)(2);

j. An award of pre- and post-judgment interest to the extent allowed by law; and

k. Such other and/or and further relief as the Court may deem proper.

COHELAN KHOURY & SINGER

Dated: December 4, 2024

By: s/*Isam C. Khoury*
Isam C. Khoury, Esq.
Attorneys for Plaintiff JOHN DEDDEH

DEMAND FOR JURY TRIAL

Plaintiff and the Class hereby demand a jury trial on all causes of action and claims with respect to which they have a right to jury trial.

COHELAN KHOURY & SINGER

Dated: December 4, 2024

By: s/*Isam C. Khoury*
Isam C. Khoury, Esq.
Attorneys for Plaintiff JOHN DEDDEH

COHELAN KHOURY & SINGER
605 C Street, Suite 200
San Diego, CA 92101